МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский ядерный университет «МИФИ»»

ЛАБОРАТОРНАЯ РАБОТА №3:
«Анализ прошивок промышленных устройств»

По предмету Информационная безопасность АСУ ТП

Выполнила студентка группы Б19-515
Щербакова Александра

Москва, 2022 г.

1 Краткое описание исследуемого устройства, его назначение

Номер в списке группы – 18. Вариант 1. Устройство – KNX Wiser.

Wiser для KNX — это логический контроллер, персонализированное решение по энергоэффективности систем домашней автоматизации, реализованное на открытых протоколах: KNX, Modbus, BACnet и IP. Контроллер Wiser для KNX может быть использован в разных сценариях:

- шлюз между KNX, Modbus, BACnet and IP
- логический модуль с функциями памяти и обработки событий
- пользовательский интерфейс через серверное web-приложение

Рис. 1 Wiser для KNX (шлюз, логический модуль, веб-сервер).

2 Анализ энтропии файла

Прошивка установлена с сайта:
https://www.se.com/id/en/download/document/FW2_7_0-HW_1_X_X-w4k/
Версия прошивки - FW2_7_0-HW_1_X_X-w4k.
Из скачанного архива интересен только сам файл прошивки - Wiser_for_KNX-2.7.0_hw1.xx.img

Расширение файла (.img) означает, что это необработанный образ тома оптического/магнитного диска.

При помощи утилиты binwalk построен график энтропии файла прошивки. Команда:
sudo binwalk -EJ Wiser_for_KNX-2.7.0_hw1.xx.img

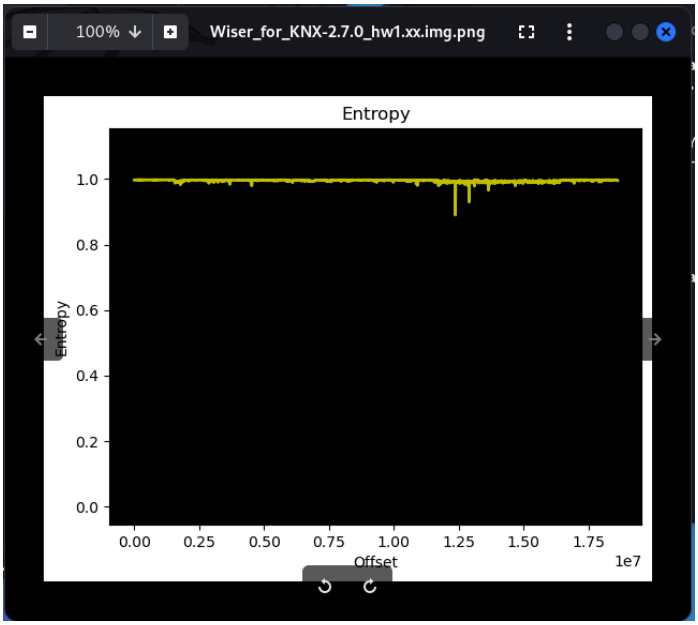

Рис 2. График энтропии файла Wiser_for_KNX-2.7.0_hw1.xx.img

Практически для всего файла энтропия близка к 1, что означает, что к файлу применено сжатие или обфускация.

3 Анализ структуры файла

При помощи утилиты binwalk проведен сигнатурный анализ файла. Команда: sudo binwalk -B Wiser_for_KNX-2.7.0_hw1.xx.img

```
┌──(aleksandra㉿kali)-[/media/sf_ib_asu_tp]
└─$ sudo binwalk -B Wiser_for_KNX-2.7.0_hw1.xx.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
1562892       0x17D90C        gzip compressed data, maximum compression, from Unix,
 last modified: 1970-01-01 00:00:00 (null date)
8960630       0x88BA76        Zlib compressed data, best compression
```

Рис 3. Сигнатурный анализ файла

Из вывода команды видно, что часть файла сжата алгоритмом gzip, а часть – Zlib, выведены смещения сигнатур относительно начала файла.

При помощи утилиты binwalk выполнено рекурсивное извлечение файлов известных типов. Пустые/неправильные файлы автоматически удалены. Команда: sudo binwalk -eMr Wiser_for_KNX-2.7.0_hw1.xx.img --run-as=root.

Папка с извлеченными файлами состоит из 526 директорий и 3171 файлов, поэтому приведена древовидная структура только до 3 уровня вложенности. Команда: tree -avd -L 3 _Wiser_for_KNX-2.7.0_hw1.xx.img.extracted

Рис 4. Структура директории извлеченных файлов

Можно заметить, что прошивка работает на базе BusyBox. В директории www хранятся файлы веб-сервера, работающего на Nginx.

3 Определение участков файла, содержащих код

При помощи утилиты binwalk выявлено, что бинарные файлы содержат инструкции архитектуры ARM и ARMEB. Команда: sudo binwalk --opcodes Wiser_for_KNX-2.7.0_hw1.xx.img

```
┌──(aleksandra㉿kali)-[/media/sf_ib_asu_tp]
└─$ sudo binwalk --opcodes Wiser_for_KNX-2.7.0_hw1.xx.img

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
2664053       0x28A675        ARMEB instructions, function prologue
4487262       0x44785E        ARM instructions, function prologue
5844278       0x592D36        ARM instructions, function prologue
11324350      0xACCBBE        ARMEB instructions, function prologue
```

Рис 4. Найденные сигнатуры исполнимых опкодов

4 Анализ архитектуры команд

Файл дизассемблирован при помощи программы IDA Pro с настройкой Processor type – ARM processors. Никакой информации о внутреннем устройстве файла это не дало.

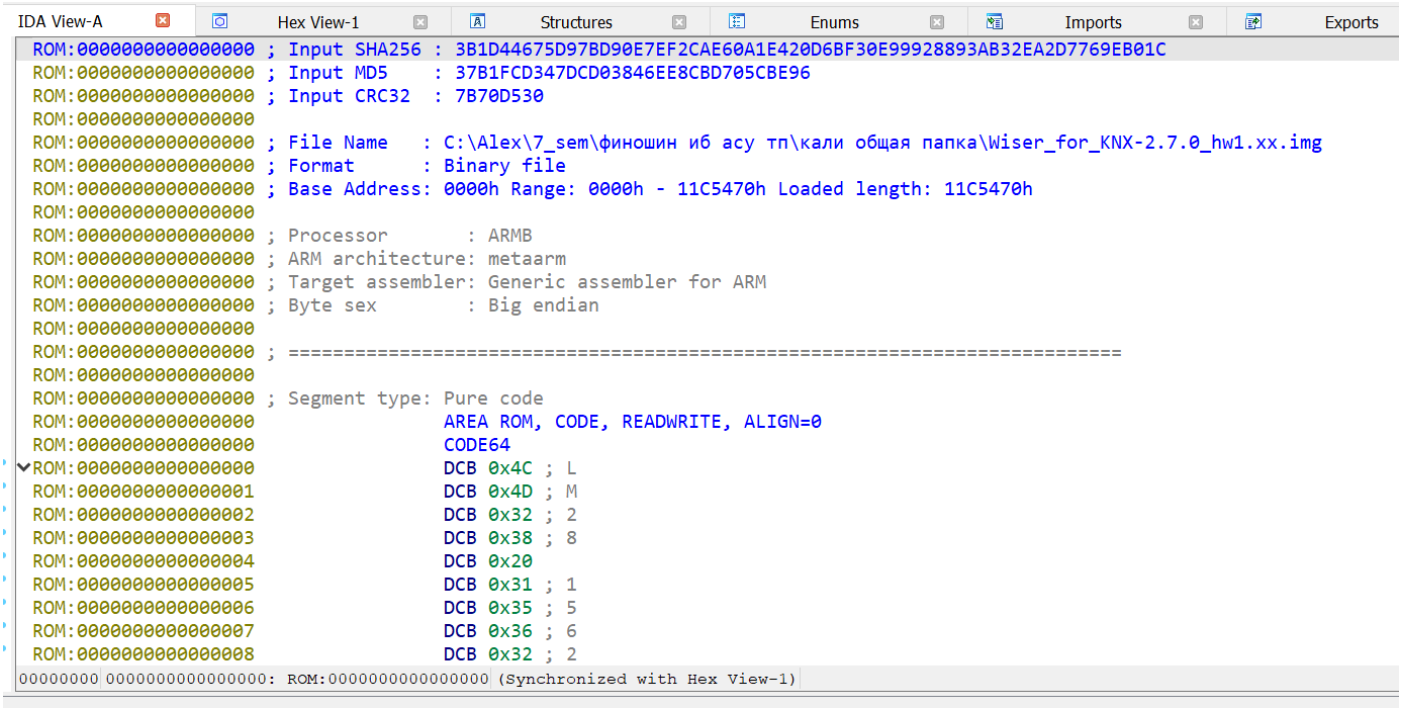

Рис 5. Дизассемблирование файла в IDA Pro

5 Поиск строк, содержащих чувствительные данные

При помощи утилит strings и grep произведен поиск читаемых человеком строк в исходном файле. Строк, содержащих чувствительные данные, не найдено.

Просмотр вывода команды strings вручную без grep также ничего не дал – все строки не содержат читаемых слов.

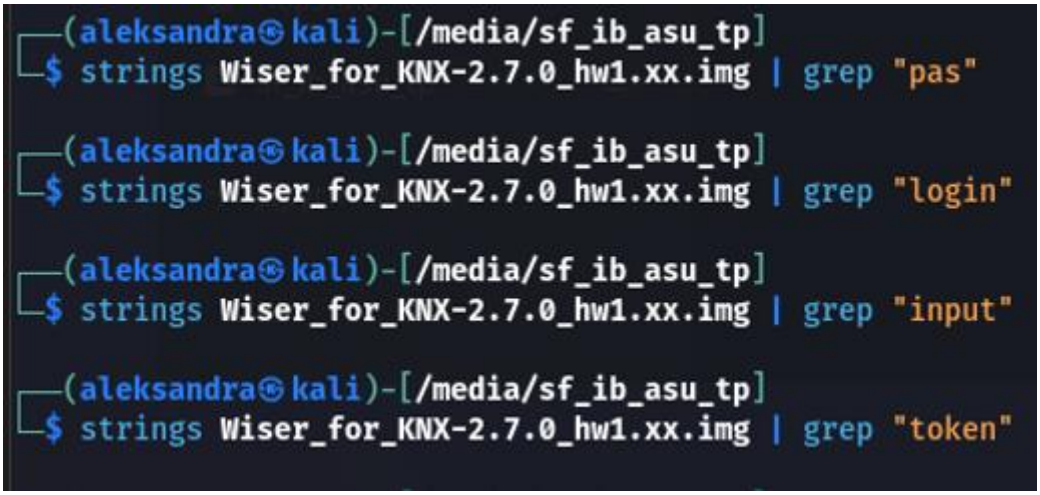

Рис 6. Поиск строк

Заключение

В ходе лабораторной работы проведен анализ прошивки промышленного устройства Wiser для KNX. Построен график энтропии файла, проанализирована структура файла. Чувствительные данные в файле не найдены.